TIETO- JA SÄHKÖTEKNIIKAN TIEDEKUNTA

Arttu Vuosku

Kotipalomuurien tietoturva

Kandidaatintyö
Tietotekniikan tutkinto-ohjelma
2021

Vuosku. (2021) Kotipalomuurien tietoturva. Oulun yliopisto, tietotekniikan tutkinto-ohjelma. Kandidaatintyö, 33 s.

TIIVISTELMÄ

Kotiverkko on herkkä kohde rikollisuudelle ja vakoilulle. Palomuuri on yksi keino suojata verkkoja virustorjuntaohjelmien ohella. Se on järjestelmä, joka sijaitsee kahden verkon rajalla ja kaiken liikenteen tulee kulkea sen läpi. Käyttäjä voi konfiguroida palomuuriin itse sopivia sääntöjä. Kotiverkon uhkia ovat madot, murtautumiset, haittaohjelmat ja palvelunestohyökkäykset. Työssä tutustuttiin erilaisiin palomuurityyppeihin ja tietoturva-aukkojen eli haavoittuvuuksien löytämiskeinoihin. Työssä testattiin pfSense-palomuuria kotikäytössä ja arvioitiin sen käytettävyyttä konfiguroimalla siihen erilaisia sääntöjä. Lisäksi etsittiin avoimia portteja oman asiakasohjelmiston avulla ja tutkittiin kotiverkon haavoittuvuuksia Nessus Essentials Vulnerability Scanner -ohjelmiston avulla. Tuloksissa huomattiin, että pfSense ei ole välttämättä helppokäyttöisin vaihtoehto kotikäyttäjälle, koska se vaatii käyttäjältä perehtymistä. Kotiverkosta ei löydetty kriittisiä haavoittuvuuksia. Työn kokeellisessa osassa selvitettiin, kuinka kotiverkkojen tietoturvaa voisi kehittää tehokkaasti ja ehkäistä mahdollisia uhkia parhaiten.

Avainsanat: palomuuri, kotiverkko, haavoittuvuus, uhka

Vuosku A. (2021) The security of home firewalls. University of Oulu, Degree Programme in Computer Science and Engineering. Bachelor's Thesis, 33 p.

ABSTRACT

Home network is a sensitive target for criminality and spying. A firewall is one way to protect networks along with anti-virus software. It is a system that is located at the barrier of two networks and all the traffic must go through it. The user can configure suitable rules to the firewall oneself. Worms, intrusions, malware and DoS (Denial of Service)- attacks are threats to home network. In the thesis, we got familiar with different types of firewalls and ways to detect vulnerabilities. PfSense firewall was tested in home usage and its usability was estimated by configurating different rules for it. Additionally, open ports were searched with own client program and Nessus Essentials Vulnerability Scanner software. In the results, it was noted that pfSense is not necessarily the user friendliest alternative for a home user, because it requires familiarization. Critical vulnerabilities were not found in the home network. It was examined, how the security of home networks could be developed effectively and prevent possible threats in the best way.

Keywords: firewall, home network, vulnerability, threat

SISÄLLYSLUETTELO

ALKULAUSE

Kiitän kandidaatintyöni ohjaajia professori Juha Röningiä, diplomi-insinööri Teemu Tokolaa sekä tietotekniikan maisteri Pekka Pietikäistä mielenkiintoisesta ja ajankohtaisesta aiheesta sekä hyvistä neuvoista ja rakentavasta ohjauksesta. Palavereissamme olen saanut erinomaisia vinkkejä työni kehittämiseen.

Haluan myös kiittää perhettäni kannustuksesta ja erityisesti isääni diplomi-insinööri Jarmo Kaikkosta tuesta työni aikana.

Oulu, maaliskuun 9. 2021

Arttu Vuosku

LYHENTEIDEN JA MERKKIEN SELITYKSET

ACK	Acknowledgment
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES-NI	Advanced Encryption Standard New Instructions
BSD	Berkeley Software Distribution
C&C	Command and Control
CGA	Cryptographically Generated Address
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DPI	Deep Packet Inspection
DS	Differentiated Services
ECN	Explicit Congestion Notification
FTP	File Transfer Protocol
Gbps	Gigabits per second
GOT	Global Offset Table
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IHL	Internet Header Length
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet Protocol, version 4
IPv6	Internet Protocol, version 6

ISO	International Organization for Standardation
LAN	Local Area Network
NAPT	Network Address and Port Translation
NAS	Network-attached Storage
NAT	Network Address Translator
Nmap	Network Mapper
NX	Non-Executable bit
P2P	Peer-to-peer
PCI	Protocol Control Information
PIE	Position-Independent Executable
RELRO	RELocation Read-Only
SDN	Software-Defined Network
SOHO	Small Office/Home Office
SPI	Stateful Packet Inspector
SSH	Secure Shell
Supo	Suojelupoliisi
SYN	Synchronized
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
VM	Virtual Machine
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WRS	Web Reputation Service

1 JOHDANTO

Keskenään yhdistettyjen laitteiden määrä kasvaa koko ajan, ja niistä muodostuu maailmanlaajuinen verkosto. Se luo ulkopuolisille mahdollisuuksia päästä käsiksi luottamuksellisiin tietoihin, joita voidaan pahimmassa tapauksessa käyttää myös rikollisiin tarkoituksiin. Tämä ongelma ei rajoitu ainoastaan yritysten verkkoihin, vaan ulottuu myös kotiverkkoihin. Tämän takia työssä tutkitaan kotiverkon palomuurien tietoturvaa ja sitä, miten niitä voidaan hyödyntää parhaiten tietoturvan edistämiseksi. Perthin Curtinin yliopistossa tehdyn tutkimuksen mukaan kotikäyttäjät ovat erityisen haavoittuvaisia tietoturvauhille. Kotikäyttäjille tarjottu tieto keskittyy lähinnä kotitietokoneisiin ja väheksyy mobiililaitteisiin kohdistuvia uhkia. [1]

Yhdysvaltalaisen CISA:n (Cybersecurity & Infrastructure Security Agency) mukaan kaksi yleistä kotikäyttäjän väärinkäsitystä ovat, että heidän kotiverkkonsa on liian merkityksetön ollakseen kyberhyökkäyksen uhrina, ja se, että laitteet ovat tarpeeksi turvallisia jo tehtaalta tullessaan. CISA suosittelee monia toimenpiteitä, joista yksi on palomuurin asentaminen verkkoon ja verkkolaitteisiin. Palomuuri paitsi suojaa ulkoisilta hyökkäyksiltä, se myös estää haittaohjelmia pääsemästä internetiin. [2]

Suomen suojelupoliisi eli Supo on havainnut autoritaaristen valtioiden tiedustelupalveluiden käyttäneen hyväksi kymmeniä suomalaisten yksityishenkilöiden ja yritysten verkkolaitteita ja palvelimia. Supo suosittelee suomalaisia tarkistamaan verkkolaitteidensa asetukset tietoturvan parantamiseksi. [3]

Työssä tutustaan aiempiin tutkimuksiin kotipalomuureista. Työssä luodaan virtuaalinen testiympäristö olemassa olevalle työasemalle palomuurien kokeilua varten ilman uusia laitehankintoja. Ympäristössä on mahdollista tutkia verkkopalomuurien toimintaa luomalla palomuurisääntöjä ja testaamalla niitä. Työssä myös tutkittiin erillisen verkkopalomuurin hyötyjä ja haittoja kotiverkossa olevien laitteiden palomuureihin verrattuna ja selvitettiin, kuinka käyttäjä voi varmistua palomuurien toiminnasta ja haittaohjelmien toiminnan estämisestä.

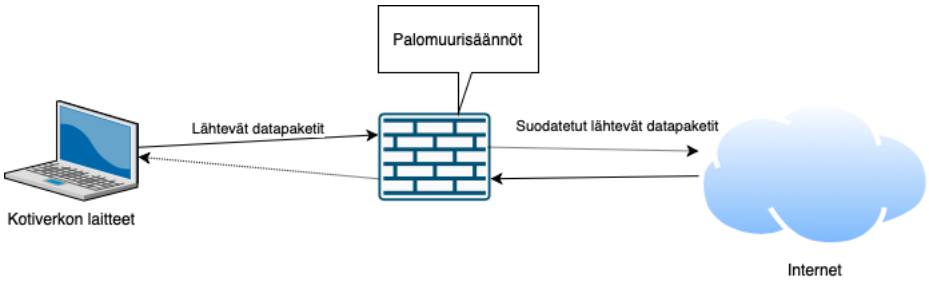
2 PALOMUURI JA TIETOTURVA

Tässä kappaleessa tutustutaan siihen mikä on palomuuri, kotiverkon rakenteeseen, internetin protokolliin, erilaisiin palomuurityyppeihin ja tietoturva-aukkojen löytämisen työkaluihin. Tämän lisäksi tutustutaan aiempiin tutkimuksiin kotipalomuureista ja kerrotaan, mitä niissä on havaittu.

2.1 Palomuuri

Käsite ”palomuuri” on vanha, sillä se on peräisin jo vuodelta 1764. [4] Nimitys tulee siitä, että muuri estää palon leviämisen rakennuksessa paikoista, joista se voi todennäköisimmin saada alkunsa, kuten esimerkiksi keittiöstä. Tietotekniikassa palomuurilla tarkoitetaan laitteita tai useampien laitteiden muodostamia kokonaisuuksia, jotka estävät ja hidastavat vaarallisten yhteyksien leviämistä tietokoneissa.

Tietotekniikassa palomuurilla on muutamia perusominaisuuksia. Palomuuri on kahden verkon rajalla ja kaiken verkkojen välisen liikenteen tulee kulkea sen läpi. Palomuurissa on mekanismi, joka valikoiden päästää liikenteen läpi tai estää sen (kuva 1). Palomuuri estää turvallisuusrikkomuksia, seuraa verkon käyttöä ja monitoroi resursseja. Palomuurissa ei ole käyttäjätilejä, eivätkä käyttäjät kirjaudu sille suoraan. Jos palomuuri vikaantuu, järjestelmä on yhä turvassa, koska liikenne ei pääse palomuurin läpi [4].



Kuva 1. Palomuurin toiminta. Internetistä tulee datapaketteja kotiverkkoon. Palomuurin säännöistä riippuen paketit joko pääsevät tai eivät pääse läpi. Käyttäjä voi itse konfiguroida sääntöjä palomuurille. Palomuuri estää myös ei-toivottua lähtevää liikennettä.

2.2 Kotiverkko

Tässä aliluvussa käsitellään kotiverkon laitteita, protokollia ja kodin IoT-laitteita.

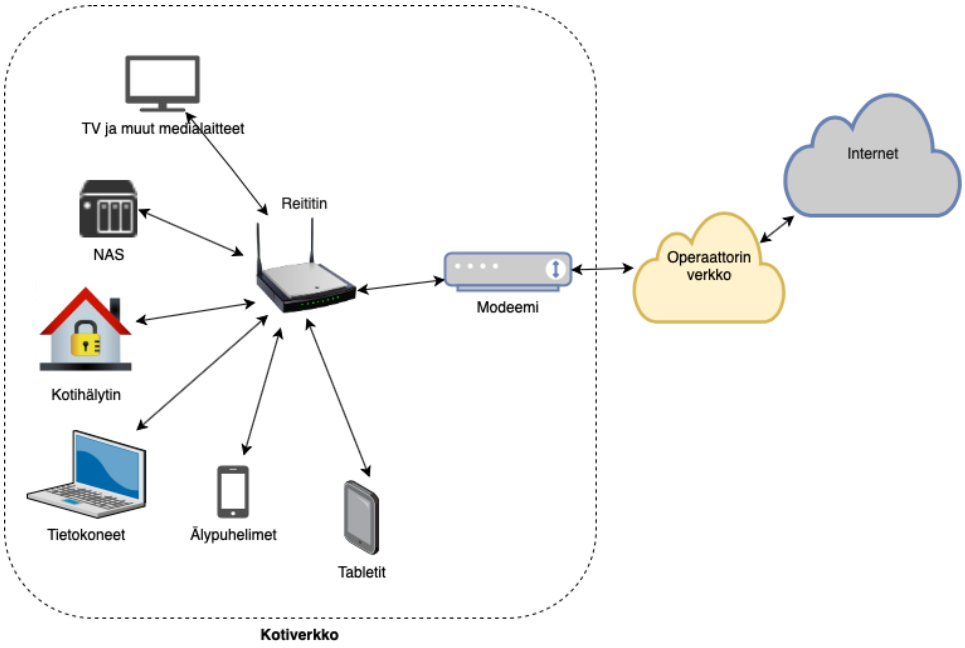
2.2.1 Kotiverkon laitteet ja liitäntä internettiin

Kotiverkko on tavallisesti yhteydessä palveluntarjoajan verkkoon laajakaistayhteydellä. Yhteys on yleisimmin toteutettu jollakin seuraavista tekniikoista:

- mobiiliverkkoon liittyvällä 4G/5G-modeemilla,

- kaapelimodeemilla,
- kotijakamoon tulevalla parikaapelilla,
- optisella kuidulla ja
- ADSL-modeemilla.

Kotiverkon ja palveluntarjoajan verkon välissä on aina reititin ja tarvittaessa modeemi. Modeemi ja reititin voivat olla samassa laitteessa ja usein reitittimet sisältävät myös langattoman (WLAN) tukiaseman. Käyttäjät voivat kytkeytyä kotiverkkoon langattomasti älylaitteella, kuten kännykällä tai tabletilla, tai sitten tietokoneiden kautta. Kotiverkkoon liittyvät myös mm. televisiot, digiboksit, tulostimet, verkkolevyasemat, mediatoistimet ja pelikonsolit. Kuvassa 2 on esimerkki kotiverkosta [5].



Kuva 2. Esimerkkejä kotiverkon laitteista.

2.2.2 Verkkoprotokollat ja NAT

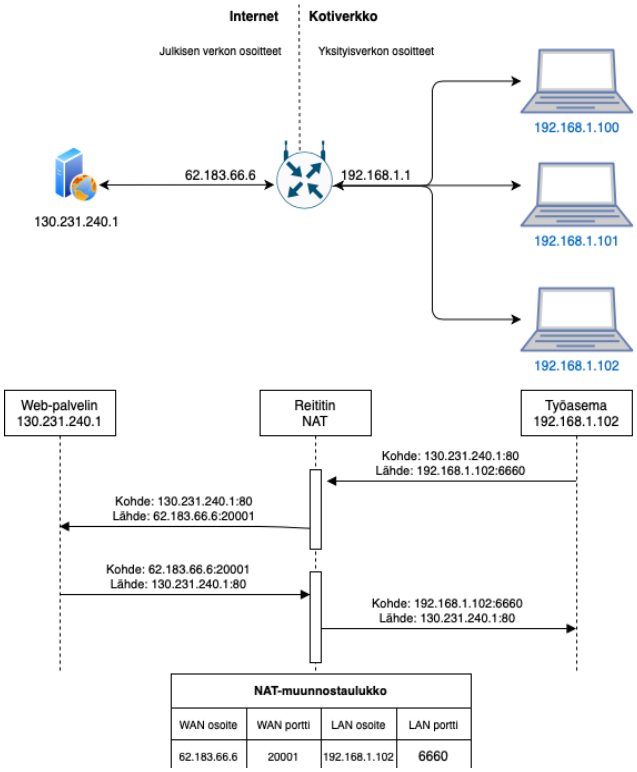
Kotiverkossa käytetään TCP/IP-protokollia. Verkkokerroksella käytössä on enimmäkseen IPv4, joka on Internet-protokollan neljäs versio. Kuitenkin kotiverkojen laitteissakin on usein IPv6-tuki ja operaattorit mahdollistavat myös IPv6-liikenteen. Palomuurien pakettisuodatus pohjautuu IP-pakettien ja TCP/UDP-sanomien kontrollitietoihin. [6]
IPv4-datagrammissa on version numero, ylätunnisteen pituus IHL(Internet Header Length), DS(Differentiated Services)/ECN(Explicit Congestion Notification) eli palvelun tyyppi, datagrammin kokonaispituus, identifiointi eli sekvenssinumero, liput joita käytetään fragmentoinnissa, fragmenttien kompensointi, joka määrittelee minne fragmentti kuuluu alkuperäisessä datagrammissa, elinaika eli datagrammin sallittu

aika Internetissä, protokolla, ylätunnisteiden tarkistussumma eli virheiden tunnistuskoodi, lähdeosoite, kohdeosoite, valinnat ja täytteet sekä data.
Palomuurissa tutkittavia kenttiä ovat ainakin protokolla (IP, ICMP, TCP, UDP yms.), lähdeosoite ja kohdeosoite. [7]

Palomuuri tutkii lähde- ja kohdeportin. Palomuurisäännön perusteella liikenne voidaan estää tai sallia määriteltyihin portteihin. Porttien lisäksi seurataan TCP-sanomissa protokollan tilaa.

UDP:ssä ei ole virheidenhallintaa, ruuhkanhallintaa eikä kättelyä palvelinten välillä. Se on tilaton protokolla, mikä estää tilaan pohjautuvan suodatuksen palomuurissa. UDP on käyttöjärjestelmästä riippumaton. [8]

NAT eli Network Address Translator on menetelmä, joka muuttaa IP-osoitteen toiseksi datagrammin ylätunnisteessa. NAT mahdollistaa yksityisverkkojen käyttäjien pääsyn maailmanlaajuiseen verkkoon muuttamalla yksityisen IP-osoitteen julkiseksi IP-osoitteeksi. Kotiverkon sisällä on yksityisverkko, jonka osoitteet eivät näy internettiin. Yksityisverkko on verkko, joka käyttää yksityistä IP-osoiteavaruutta. Yksityisverkon osoitteet ovat 192.168.0.0/16, 10.0.0.0/8 ja 172.16.0.0/12. Perus-NAT suorittaa osoitemuunnoksen yhden yksityisen ja yhden julkisen IP-osoitteen välillä, kun taas NAPT (Network Address and Port Translation) suorittaa sen yhden julkisen ja monen yksityisen IP-osoitteen välillä. NAT:ista on hyötyä kotiverkon suojauksessa: Se estää ulkoiset hyökkäykset ja kontrolloi sisäisten palvelimien pääsyä ulkoisiin verkkoihin sekä ulkoisten käyttäjien pääsyä sisäiseen verkkoon. [7] NAT ei kuitenkaan estä kotiverkon laitteella olevan haittaohjelman toimintaa, jos haittaohjelma avaa yhteyksiä kotiverkosta internettiin. Portinsiirtotoiminnolla on myös mahdollista määritellä julkiseen osoitteeseen liittyvä portti, joka reititetään haluttuun kotiverkon osoitteeseen ja porttiin. Kuvassa 3 on esimerkki NAT-muunnoksesta [9].



Kuva 3. Esimerkki NAT-muunnoksesta. Osoitteen muutokset näkyvät muunnostaulukossa.

2.2.3 IoT-laitteiden turvallisuus

Kodin verkkolaitteisiin kuuluu IoT-laitteita (Internet of Things) eli laitteita, jotka muodostavat yhteyden internettiin ja siirtävät tietoa sen läpi. Yksi suurimpia haasteita nykyisissä IoT-laitteissa on se, että ne eivät välttämättä ole turvallisia, koska turvallisuusprotokollasta puuttuvat tärkeät turvallisuusominaisuudet ja luottamus laitteiden välillä on olematon. Suurimpia haavoittuvuuksia IoT-laitteissa on heterogeeninen arkkitehtuuri, vanhentuneet protokollat, heikko enkryptaus, rajallinen muisti, epäturvalliset sovellukset, heikko tunnistautuminen ja sulautettujen ohjelmien viat. IoT-laitteiden yleisimmät uhat ovat palvelunestohyökkäykset, salakuuntelut, toisena henkilönä esiintymiset ja turvallisuusrikkomukset. IoT-laitteiden turvallisuutta voi parantaa palomuurien ja ohjelmiston päivittämisen avulla. Ne ovat tärkeitä asioita turvallisuuden varmistamisessa. Muita keinoja IoT-laitteiden suojaamiseen ovat tehokas enkryptaus, yksityinen verkko, ajantasaiset protokollat, pääsytietojen vaihtaminen, tärkeiden tietojen varmuuskopiointi ja verkon monitorointi. [10]

2.3 Palomuurien toiminnallisuus

Tässä aliluvussa tarkastellaan palomuureja käytännössä.

2.3.1 Palomuurityypit

Palomuureja on kolme eri tyyppiä: pakettisuodatin, sovelluskerroksen palomuuri ja tilallinen pakettisuodatin.

Pakettisuodatin (tästä käytetään myös termiä tilaton pakettisuodatin) on toteutettu siten, että palomuuri tutkii jokaisen datapaketin ja vain asetettuja kriteerejä vastaavat paketit pääsevät läpi. Pakettisuodatin estää kaiken, mikä ei ole erikseen sallittu. Sillä on sisäänpääsylista paketeista. Pääsylistaa kutsutaan myös nimellä ACL (Access Control List).

Tilallinen pakettisuodatin eli SPI (Stateful packet inspector) tutkii paketit kuten tavallinen pakettisuodatin, mutta tutkinta ei perustu ainoastaan tietyn hetkisen paketin tutkimiseen, vaan myös edellisten pakettien sisältämiin datoihin. [11]

Tilallista pakettisuodatusta käytetään esimerkiksi TCP-protokollaan. TCP:ssä asiakas lähettää palvelimelle datapaketin, minkä avaussanoma on SYN ja palvelin vastaa SYN-ACK-viestillä, että se on vastaanotettu. Sen jälkeen asiakas lähettää kuittauksen vastauksesta, mitä kutsutaan ACK-sanomaksi (acknowledgment). SPI-palomuuri pitää kirjaa lähetetyistä viesteistä tilataulukossa. Se tarkistaa lähde-IP:n ja -portin, kohde-IP:n ja -portin sekä TCP-protokollan tilan SYN-SENT, SYN-ACK-SENT, ACK-SENT, established) ja hyväksyy vain tilataulukon ja palomuurisääntöjen perusteella sallitut TCP-viestit. [6, 12]

Sovelluskerroksella toimivat palomuurit voivat estää kaikkien pakettien kulkemisen sovelluksesta toiseen. Sovelluskerroksen palomuuri neuvottelee erilaisten sovellusten kanssa niiden liikenteen päästämisestä läpi. [11]

Palomuurit voidaan jakaa myös päätelaitekohtaisisiin (host-based firewall) ja verkkopalomuureihin (network firewall), jotka eroavat toisistaan monilla tavoilla. Päätelaitekohtainen palomuuri sopii yhden tietokoneen tai pienen lähiverkon suojaksi ja soveltuu kotikäyttäjille. Päätelaitekohtainen palomuuri voi olla tietokoneelle asennettava ohjelma. Puhutaan myös henkilökohtaisista palomuureista (personal firewall), joka tarkoittaa käytännössä samaa asiaa kuin päätelaitekohtainen palomuuri. Verkkopalomuuri suojaa koko verkkoa ja on tarkoitettu verkon ylläpitäjille. Kotiverkossa verkkopalomuurin toiminnallisuus voi sisältyä modeemeihin, reitittimiin tai erillisiin palomuurilaitteisiin. [13]

2.3.2 Tunkeilijan havaitsemis- ja estojärjestelmät

IDS (Intrusion Detection System) eli tunkeilijan havaitsemisjärjestelmä ja IPS (Intrusion Prevention System) eli tunkeilijan estämisjärjestelmä ovat osa verkon infrastruktuuria. IDS on ylläpitojärjestelmä, kun taas IPS on hallintajärjestelmä. IDS ei muuntele datapaketteja, mutta IPS estää paketin jakamisen paketin sisältämän datan perusteella. IDS on työkalu, joka ylläpitää ja analysoi tietoliikennettä kyberuhkien varalta. IPS on samalla alueella kuin palomuuri, eli ulkomaailman ja sisäisen verkon välissä. Se estää liikenteen pääsyn, mikä perustuu paketin turvallisuusprofiiliin.

Sekä IDS ja IPS ovat tärkeitä kyberturvallisuudessa, koska ne auttavat turvallisuuskäytäntöjen soveltamisessa. Ne toimivat verkossa ja palvelimessa ja niitä käytetään sensoreina. Sellainen voi olla jokin seuraavista laitteista: IPS- ohjelmistolla konfiguroitu reititin, IDS- tai IPS-palvelujen tarjoamiseen erityisesti suunniteltu laite tai verkkomoduuli, joka on asennettu laitteeseen, kytkimeen tai reitittimeen. Näiden ero palomuuriin on siinä, ettei palomuuri analysoi liikenteen mallia. Lisäksi palomuuri sallii ja estää liikennettä protokollasäännön, IP-osoitteiden, porttinumeroiden ja

verkkoyhteyden tilan perusteella, kun taas IDS ja IPS havaitsevat säännöttömästi. IDS ja IPS nostavat myös hälytyksen, kun taas palomuuri ei sitä tee.

IDS:llä ja IPS:llä on neljä järjestelmätyyppiä: tunnisteperusteinen, käytäntöperusteinen, epäsäännöllinen ja ”hunajapurkki”-perusteinen. Tunnisteperusteinen järjestelmä vertailee ennalta määriteltyjä tietoliikenteen malleja tunnettuihin hyökkäyksiin. Jos niiden välillä on vastaavuus, järjestelmä nostaa hälytyksen. Tunniste voi perustua joko yksittäiseen pakettiin tai pakettijonoon. Käytäntöperusteisessa järjestelmässä on ennalta määrätty käytäntö, johon sensorin konfigurointi perustuu. Käyttäjän on itse luotava käytäntö. Kaikki käytännön ulkopuolinen liikenne nostaa hälytyksen tai sitten se estetään. Epäsäännöllinen järjestelmä etsii tietoliikennettä, joka poikkeaa ”normaalista”. Tässä yhteydessä ”normaali” tulee määritellä itse. Siinä on ongelma, jos järjestelmä pitää hyökkäystä normaalina, ja järjestelmä ei hälytä siitä, kun se tapahtuu uudelleen. ”Hunajapurkki-järjestelmässä” yritetään houkutella hyökkääjiä. Niitä houkutellaan pois oikeista verkkolaitteista. Tällä menetelmällä voidaan analysoida hyökkäysten ja vaarallisen liikenteen malleja. Analyysin perusteella voidaan virittää sensoritunnisteet havaitsemaan uudentyyppistä vaarallista tietoliikennettä. [14]

2.3.3 Palomuurin torjumat uhat ja rajoitukset

Palomuurit suojaavat tietojärjestelmää madoilta, murtautumisilta, haittaohjelmilta ja palvelunestohyökkäyksiltä. Haittaohjelmat, joihin kuuluvat Troijan hevoset, virukset ja vakoiluohjelmat, ovat yleisin uhka tietokoneelle. Troijan hevonen on viattomaksi naamioitu haittaohjelma, joka tekee hyödyllisen toiminnon käynnistäen samalla viruksen tai madon, tehden tuhoja tai avaten haavoittuvuuden tietojärjestelmään. Troijan hevonen voi myös liittää tietokoneen osaksi bottiverkkoa. Bottiverkoista kerrotaan tarkemmin kappaleessa 2.5.4.

Virus on tietokoneohjelma, joka monistaa itseään ja leviää toisiin tietokoneisiin. Vakoiluohjelma on haittaohjelma, joka kerää tietokoneesta ja sen käyttäjästä tietoa ilman käyttäjän suostumusta ja välittää ne toiselle taholle. Mato on itsenäinen ohjelma, joka hyökkää järjestelmään ja yrittää hyödyntää sen haavoittuvuutta. Sen jälkeen se kopioi ohjelmaansa isännästä uuteen järjestelmään käynnistääkseen syklin uudelleen. Palvelunestohyökkäyksessä estetään palvelun käyttö kohdistamalla verkkosivulle niin paljon liikennettä, ettei se pysty palvelemaan asiakkaitaan. Se voi olla myös tietojen poistamista tai korruptoimista. [15]

Palomuurilla on monia rajoituksia. Se ei voi estää modeemilla varustettuja käyttäjiä eikä hyökkääjiä ottamasta yhteyttä sisäiseen verkkoon tai sieltä muualle. Lisäksi se ei voi soveltaa salasanakäytäntöjä tai ehkäistä salasanan väärinkäyttöä. Palomuuri ei voi estää käyttäjiä - ellei sitä ole sitä varten erikseen konfiguroitu - menemästä internet-sivuille, joista voi saada viruksia eikä myöskään suojata huonoilta päätöksiltä. Palomuuri ei siis ole sama asia kuin virustorjuntaohjelma. [16]

2.3.4 Kotikäyttäjän henkilökohtaiset palomuurit

Henkilökohtaisen palomuurin kotikäyttäjä voi saada käyttöönsä joko työaseman (tietokoneen) käyttöjärjestelmän mukana tai hankkimalla erillisen tietoturvaohjelmiston, jossa on virustorjunnan lisäksi palomuuriominaisuus.

Windowsissa on Windows Firewall, joka on palomuurisovellus. Se suodattaa Internetistä tulevaa tietoliikennettä ja estää haitalliset ohjelmat. Windows Firewallissa on pääsylista sallituista ohjelmista. Se estää kaikki pyytämättömät yhteydet tietokoneeseen. [17]

MacOS:n palomuuri on ohjelmapalomuuri, joka toimii käyttöjärjestelmän 10.5.1-versiossa ja uudemmissa versioissa. Siihen voi määrittää palomuurisäännöt. Siinä on myös lisäasetuksia, kuten kaikkien saapuvien yhteyksien estäminen ja tiettyjen ohjelmien salliminen. [18]

Linux-jakeluissa on kaksi erilaista palomuuritoteutusta: iptables ja firewalld. Molempien konfigurointi toimii komentoriviltä. Iptablesilla konfiguroidaan suodatussäännöt Linux-kernelin palomuurille. Iptablesilla konfiguraation muutos aiheuttaa kaikkien sääntöjen uudelleenlatauksen ja olemassa olevien yhteyksien katkaisun. Firewalld:lle määritellään internet-yhteyksien ja -rajapintojen luotettavuustaso. Firewalld:ssä on mahdollista määritellä uusia sääntöjä ajon aikana ilman että olemassa olevia yhteyksiä katkotaan. [19, 20, 21]

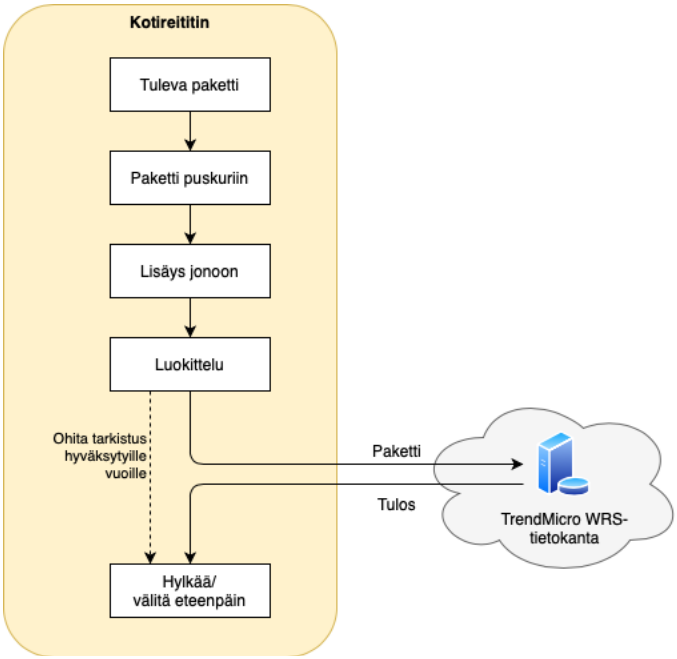
2.3.5 Kotiverkon verkkopalomuurit

Verkkopalomuurit ovat laitteita, jotka pysäyttävät tai vähentävät vahvistamatonta liikennettä, joka yrittää päästä yksityisverkkoon. Sallittava liikenne määritellään palomuurikäytäntöjen kautta. Ne sijaitsevat ulko- ja sisäverkon välissä ja toimivat ulkoisten ja sisäisten laitteiden yhdistäjinä. Verkkopalomuurit ovat tärkeitä, sillä ilman niitä yksityisverkot voivat olla helpompia kohteita hyökkäyksille. Kaikissa kodin verkkoon liittyvissä laitteissa ei ole omaa palomuuria ja verkkopalomuuri on ainoa keino suojata niitä.

2.3.5.1 Reitittimissä olevat valmiit palomuuriominaisuudet

Kotireitittimiin sisältyy tavallisesti SPI-palomuuri, jolla voi suodattaa lähtevää ja tulevaa liikennettä. Palomuurissa voi olla käytettävissä URL-suodatus, avainsana-suodatus salaamattomien Web-sivujen tietosisällön perusteella tai tiettyjen verkkopalvelujen esto ajastetusti.

Joihinkin reitittimiin on toteutettu myös syvällisempää pakettien sisällön tutkintaa ja IDS/IPS-ominaisuuksia. Esimerkki tästä on ASUS:in reitittimistä löytyvä AiProtection, joka etsii reitittimen asetuksista vaarallisia porsaanreikiä ja poistaa haavoittuvuuksia. Lisäksi se estää käyttäjää vierailemasta vaarallisilla internet-sivuilla. Kolmanneksi AiProtection vähentää erilaisten kyberuhkien tunkeutumista kotiverkkoon. AiProtection käyttää DPI-menetelmää (Deep Packet Inspection), joka tutkii pakettien sisällön. Kuvassa 8 on esitetty DPI:n toimintaa: paketit tarkistetaan ulkoisessa Web Reputation Service (WRS) -palvelussa ja tämän tarkistuksen perusteella pääsy jollekin Web-sivulle joko sallitaan tai estetään reitittimellä. [22]



Kuva 4. DPI-menetelmä ASUS-reitittimissä

2.3.5.2 Itse rakennettavat palomuurit

Palomuureihin perehtyneen kotikäyttäjän on mahdollista rakentaa oma palomuuri yleiskäyttöisistä tietokoneista ja avoimen lähdekoodin palomuuritoteutuksista. Tässä on joitakin esimerkkejä [23]:

IPFire on avoimen lähdekoodin palomuuri, joka perustuu Linuxiin. Se on helppokäyttöinen ja sillä on korkea suorituskyky. Turvallisuus on IPFiren korkein prioriteetti. Sillä on tunkeutumisenjäljitysjärjestelmä, joka analysoi verkkoliikenteen ja yrittää löytää hyväksikäyttöjä, vuotavaa dataa ja muita epäilyttäviä toimia. Sitten se käynnistää hälytyksen ja estää tunkeilijan. IPFireen voi myös asentaa lisäominaisuuksia: IPFiren muuttaminen tukiasemaksi, työkalut monitorointiin ja systeemin kunnon ylläpitoon, varmuuskopio-, tiedosto- ja tulostuspalvelut, Tor-solmun ajaminen, proxyt ja relet eli kytkimet eri protokollille sekä monia muita.

PfSense on ilmainen avoimen lähdekoodin palomuuri, joka perustuu FreeBSD-käyttöjärjestelmään. Se on saatavilla laitteistona, virtuaalilaitteena ja ladattavana binäärikoodina.

OPNSense on PfSensen ja m0n0nwallin haara. Siinä on kahden tekijän tunnistautuminen ja sitä päivitetään säännöllisesti.

Smoothwall-palomuurissa on yksinkertainen rajapinta, josta voi ylläpitää palomuuria. Ufw toimii Ubuntussa. Siinä on komentorivirajapinta verkkosuodattimen ylläpitoa varten. Csf on tilaton pakettisuodatin, joka toimii Linux-palvelimissa.
Lisäksi kaupallisista palomuureista saa kotikäyttöön soveltuvia versioita, jotka voi asentaa valitsemaansa laitteistoon. Esimerkki kaupallisesta palomuurista on Sophos.

Avoimen lähdekoodin palomuurit – kuten pfSense ja IPFire – voi saada toimimaan IDS/IPS roolissa sopivilla lisämoduuleilla kuten Snort tai Suricata.

2.4 Tietoturva-aukkojen löytäminen

Tietoturva-aukoilla tarkoitetaan ohjelmistoissa tai laitteissa olevia virheitä, joiden avulla ulkopuolinen voi päästä tietojärjestelmään.

Penetraatiotestaus on menetelmä, jolla tietoturva-aukkoja yritetään löytää ja saada varmuus tietojärjestelmän suojausten asianmukaisuudesta hyökkäyksiä vastaan. Penetraatiotestaukseen on olemassa useita erilaisia työkaluja ja osa niistä soveltuu myös kotiverkon ja siinä käytössä olevien palomuurisääntöjen tarkistukseen.

Vuonna 2004 julkaistu Metasploit on yksi esimerkki niistä. Metasploit Framework on ilmainen ja yleisesti käytetty testausohjelma, jolla on avoin lähdekoodi. Siitä on olemassa myös ammattilaisversio. Metasploitilla voi suorittaa penetraatiotestauksen esimerkiksi verkkoversiona, mikä on automaattinen, tai konsoliversiona, mikä muistuttaa komentoriviä ja on manuaalinen. Metasploit oli käytössä eräässä Michael D. Mooren tekemässä yhdysvaltalaistutkimuksessa Metasploitable 2:n penetraatiotestauksessa. Metasploitable 2 on Linux-pohjainen käyttöjärjestelmä. [24, 25]

Nessus Solutions on Tenablen kehittämä sarja työkaluja tietoturva-aukkojen löytämiseen. Nessus Essentials on mahdollista ladata kotikäyttöön ilmaiseksi – muut tuotteet ovat ammattikäytöön tarkoitettuja. [26]

Nmap on ilmainen ja avoimen lähdekoodin työkalu verkon laitteiden löytämiseen ja turvallisuuden tarkastamiseen. Se käyttää käsittelemättömiä (raw) IP-paketteja ottaakseen selvää siitä mitkä päätteet ovat saatavilla ja mitä palveluja ne tarjoavat, mitä käyttöjärjestelmiä ne käyttävät, minkälaisia paketinsuodattimia tai palomuureja on käytössä ja lukuisista muista ominaispiirteistä.

Metasploitissa on verkon laitteiden läpikäynti (discovery scan), joka käyttää Nmappia TCP-porttien havaitsemiseen ja pyörittää havainnoinnin lisämoduuleja kerätäkseen lisätietoja kohdepäätelaitteista. Löydön havaitsemisessa on neljä vaihetta: pingaaminen (laitteen havaitseminen), portin havaitseminen, käyttöjärjestelmän ja version skannaus ja datan tuominen. Pingaamisessa selvitetään, ovatko päätteet saatavilla. Porttien havaitseminen tarkoittaa, että selvitetään saatavilla olevat palvelut porteissa. Kolmannessa vaiheessa Nmap lähettää tarkistussanomia avoimille porteille ja selvittää palveluiden versionumerot ja käyttöjärjestelmän vastausten perusteella. Ne tarjoavat arvokasta tietoa järjestelmästä. Lopuksi Nmap kerää kaiken datan ja tekee raportin. [27] Penetraatiotestaus ei ole välttämättä helppoa asiaan vähän perehtyneille. Se vaatii paljon tutustumista. Lisäksi penetraatiotestaajan on oltava eettinen testauksen aikana ja sen jälkeen. [28,29]

2.5 Kotipalomuureihin liittyviä tutkimuksia

Tässä aliluvussa käsitellään tutkimuksia kotipalomuureista.

2.5.1 Palomuurien käytettävyys

Karlstadin yliopistossa tehdyssä tutkimuksessa [30] todettiin, että palomuurin helppo konfiguroitavuus on kotikäyttäjälle erittäin tärkeää, jotta tietoturvaominaisuudet tulisivat kunnolla käyttöön. Tutkimuksen mukaan käyttäjien ja suunnittelijoiden näkemykset henkilökohtaisista palomuureista eroavat kuitenkin paljon toisistaan.

Palomuurien suunnittelun ja toteutuksen tulisi tapahtua käyttäjävaatimusten perusteella, minkä vuoksi käytön evaluointi on tärkeää. Tutkimuksen perusteella palomuurin toteuttajille suositellaan palomuurin näkyvyyden parantamista käyttäjälle, käytön oppimiseen rohkaisemista ja luodun säännön selkeää esitystä kuin myös opastusta siitä, mitä käyttöliittymässä on tehtävä. Tämä tarkoittaa myös varoittamista vaarallisista toimenpiteistä.

Tärkeää on myös vähimmän käyttöoikeuden periaate ja hätäisesti tehtyjen päätösten helppo korjattavuus jälkikäteen. Tutkimuksessa todettiin sääntöjen visualisoinnin olevan tehokkaampaa tekstin sijaan, koska se auttaa käyttäjää ymmärtämään säännöt helpommin. Sääntöjen väärin konfigurointia ei tulisi tapahtua, koska se voi lisätä verkon haavoittuvuutta, kuten myös hajautetut ja useat palomuurit. Tutkimuksen mukaan verkkopalomuurien konfigurointi on monimutkaisempaa kuin henkilökohtaisten palomuurien.

2.5.2 Kotiverkon reitittimien haavoittuvuudet

Kotiverkossa palomuuri on usein toteutettu reitittimen sisäänrakennetuilla palomuuriominaisuuksilla eikä käytössä ole erillistä verkkopalomuuria.
Fraunhofer-instituutin tutkimuksessa [31] selvitettiin kotiverkon reitittimien virheitä. Tutkimuksessa esitettiin viisi kysymystä:

- Milloin reititin viimeksi päivitettiin?
- Mitä käyttöjärjestelmäversioita käytettiin ja kuinka monta tunnettua haavoittuvuutta vaikuttaa niihin?
- Mitä haavoittuvuuksien estämiskeinoja laitevalmistajat käyttävät ja kuinka usein he aktivoivat ne?
- Sisältävätkö sulautettujen järjestelmien ohjelmistot yksityisavaimia?
- Onko mitään kovakoodattuja kirjautumisen pääsytietoja?

Tutkituista 127 reitittimestä 81 reititintä oli päivitetty vuoden sisällä, 22 reitittimessä päivitys oli yli kaksi vuotta vanha ja pahimmassa tapauksessa päivitystä ei ollut tehty yli viiteen vuoteen. Yleisin käyttöjärjestelmä oli Linux, josta yli kolmasosassa laitteita oli käytössä versio 2.6.36 tai sitä vanhempi versio. Tutkimuksessa analysoitiin seuraavaa viittä eri keinoa, joilla voidaan estää haavoittuvuuden hyväksikäyttöä.

- NX eli ei-suoritettava bitti estää hyökkääjää suorittamasta koodiaan merkitsemällä uhrin muistin osia ei-suoritettaviksi.
- Sijainnista riippumaton suoritettava koodi eli PIE (Position-Independent Executable) satunnaistaa sallittujen ohjelmien ja kirjastojen koodien sijainnin, ettei hyökkääjä voi löytää niitä käyttäjän muistista.
- RELRO (RELocation Read-Only) suojelee GOT-muistia (Global Offset Table) manipuloinnilta ohjelman suorituksen aikana.
- Pino-canaryt eli ”kanarianlinnut” estävät ylivuotohyökkäyksiä siten, että ne tallentavat erityisiä bittisekvenssejä muistiin. Niitä tarkistetaan muutosten varalta ohjelman suorituksen aikana. Ilman tarkistusta hyökkääjä voi suorittaa oman koodinsa ohjelman suorituksen aikana.
- FORTIFY_SOURCE on merkkijono-operaatio, joka rajoittaa datan pituuden enimmäismäärää.

Haavoittuvuuksien hyväksikäytön estämiskeinoja käytettiin harvoin lukuun ottamatta NX:ää, jota käytettiin lähes kaikkien laitetoimittajien kaikissa laitteissa. Keskimäärin viisi yksityisavainta julkaistiin yhdessä sulautetun järjestelmän ohjelmistossa, mutta esimerkiksi Netgear R6800 tarjoaa 13 yksityisavainta. Yli 60 %

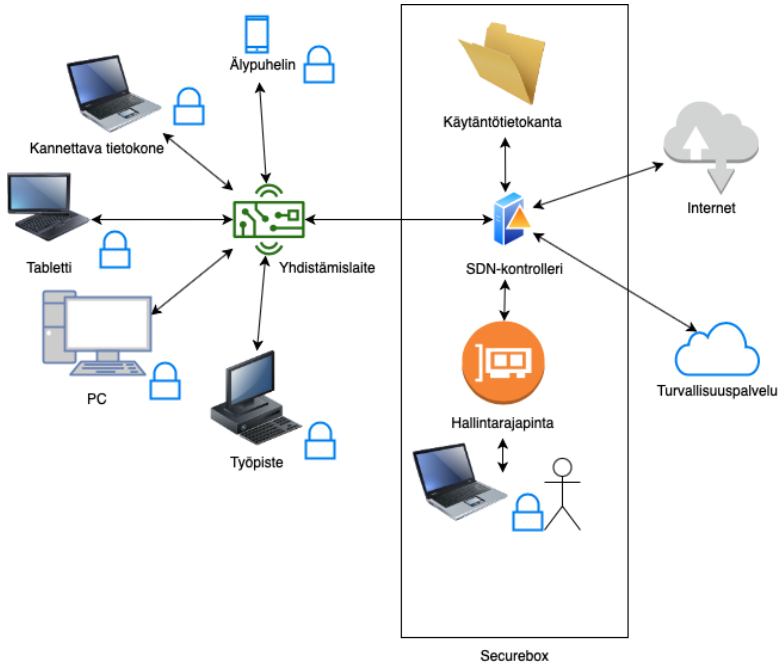
sulautetuista järjestelmistä ei sisältänyt pääsytietoja, kuten käyttäjätunnuksia ja salasanoja. Tutkimus osoitti myös, että turvallisuusanalyysi voidaan tehdä vain avoimen lähdekoodin ohjelmistoille.

Jerusalemin yliopistossa tehdyssä tutkimuksessa [32] tutkittiin Small Office/Home Office (SOHO) -reitittimien haavoittuvuuksia. Tietoa kerättiin lähettämällä pyyntöjä palvelimille, jotka käyttivät urllib-kirjastoa. Reitittimien ongelmat jaettiin kahteen luokkaan: toisissa oli haavoittuvainen vahvistusrajapinta, josta puuttuvat pääsytiedot, ja toiset käyttävät oletuspääsytietoja. Tutkimuksen alussa tunnistettiin reitittimen tyyppi. Tutkimuksessa havaittiin, että 90 prosenttia avoimista laitteista on SOHO-laitteita ja loput web-kameroita, ja että pelkästään verkkolaitteiden tiedusteleminen herättää eettisiä kysymyksiä. Osa haavoittuvuuksista johtuu käytännöistä. Esimerkiksi lainsäädäntö ei valvo internet-palveluntarjoajien vastuuta SOHO-laitteiden valvonnasta.

2.5.3 Securebox-laite

Helsingin yliopiston, Münchenin teknisen yliopiston ja F-Securen tutkimuksessa on esitetty Secureboxia edulliseksi ratkaisuksi asioiden internetin (Internet of Things, IoT) turvallisuuteen. Ratkaisua esitettiin, koska mobiili- ja IoT-laitteiden määrä kasvaa koko ajan ja ne tuovat käyttäjille uuden tyyppisiä tietoturvauhkia, jotka koskevat dataa, laitteiden turvallisuutta ja käyttäjän yksityisyyttä. [33]

Securebox on muunneltu yhdyskäytävä, joka ajaa SDN-kontrolleria ja OpenVSwitchiä. Siinä on oma tietokanta tietoliikenteiden turvallisuuskäytännöille. Securebox tarjoaa langallisia ja langattomia rajapintoja käyttäjälaitteiden yhdistämiseen. Kaikki lähtevä ja tuleva liikenne kulkee Secureboxin läpi. [34] Kuvassa 9 on Secureboxin arkkitehtuuri.



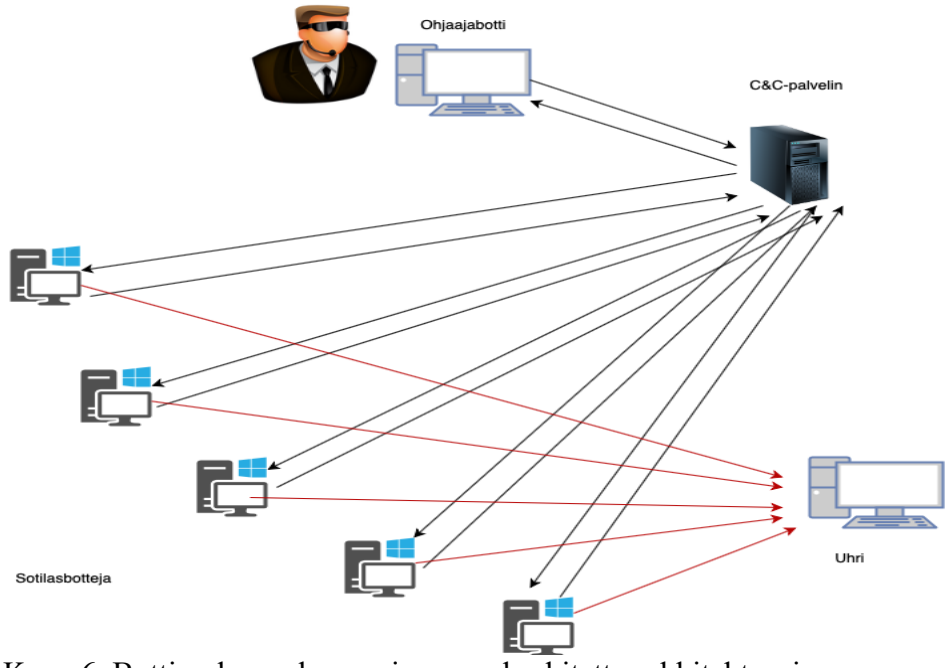
Kuva 5. Secureboxin arkkitehtuuri

2.5.4 Palomuuri ja bottiverkot

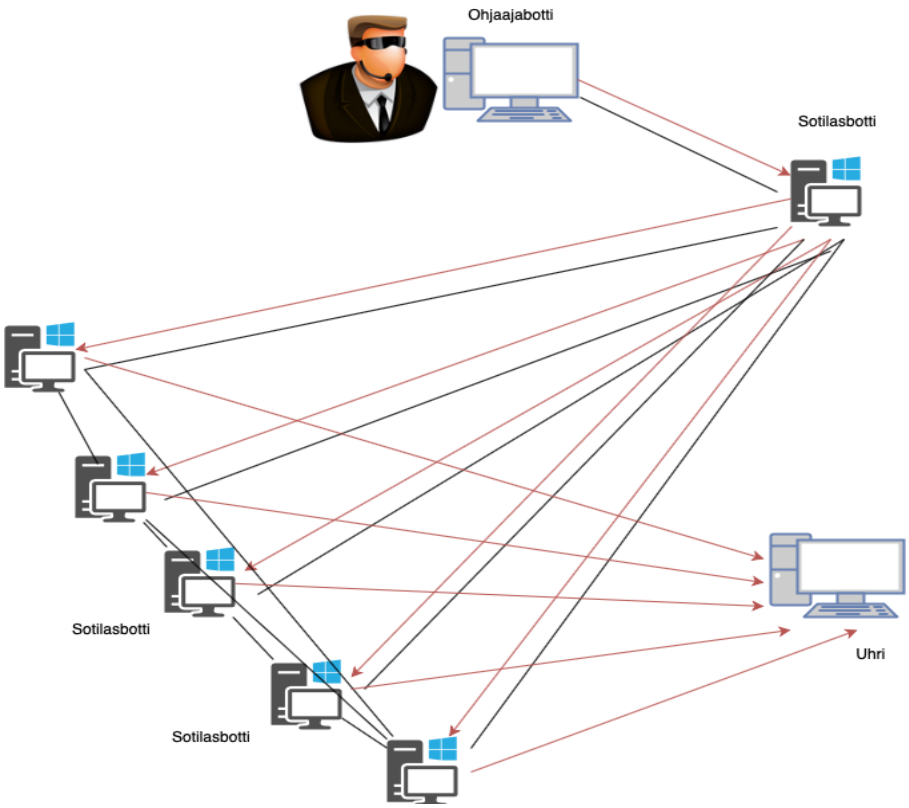
Bottiverkot koostuvat tietokoneohjelmista, jotka ovat yhteydessä toisiinsa tietoverkon kuten internetin välityksellä. Ne eivät ole vain uhka tietokoneverkolle, vaan niitä käytetään myös pahantahtoisiin tarkoituksiin kuten palvelunestohyökkäyksiin, sen takia niiden monipuolisuus on mielenkiintoinen mutta vaarallinen. Bottiverkkoja käytetään myös henkilökohtaisen tiedon keräämiseen ”rikollismarkkinoilla” myytäväksi. Muita uhkia ovat klikkivilppi (click fraud) ja laiton verkkoisännöinti (illegal hosting).

Bottiverkko toimii siten, että se aluksi saastuttaa toisen tietokoneen. Sitten se injektoi koodinpätkän käyttämällä tiedostonsiirtoprotokollaa (FTP, File Transfer Protocol), hypertekstinsiirtoprotokollaa (HTTP, Hypertext Transfer Protocol), vertaisverkkoa (P2P) ja HTTP:n ja P2P:n yhdistelmää (HTTPP2P). Kun käyttäjä yhdistää internettiin, koodia suoritetaan yhteyden muodostamiseksi C&C (Command and Control) -palvelimelle. Ohjaajabotti komentaa ja ohjaa niin sanottuja ”zombikoneita” C&C-palvelimen kautta. Ohjaajabotti pysyy läpinäkyvänä ja aktiivisena käyttämällä dynaamista nimipalvelua ja päivittää ”zombikoneita” ja pitää niitä toiminnassa ylläpitääkseen niitä ja käyttääkseen niitä sen mukaisesti.

Bottiverkkojen estämiskeinoja ovat virustorjuntaohjelmat, salasanan päivitys, ohjelmiston päivitys, palomuuri, UPnP:n (Universal Plug and Play) kytkeminen pois päältä ja tunkeilijan estämisjärjestelmä eli IPS. Kaikki käytetyt tekniikat, mukaan lukien palomuuri, eivät välttämättä ole sovellettavissa uuden sukupolven bottiverkkoihin. Sen vuoksi tiedonlouhintaan ja DNS-liikenteen bottiverkon C&C-havaitsemiseen perustuvien tekniikoiden löytäminen voisi olla hyvä lähestyminen uhkien torjumiseen tietokoneresursseissa. [35, 36]



Kuva 6. Bottiverkon rakenne, jossa on keskitetty arkkitehtuuri.



Kuva 7. Bottiverkon rakenne, jossa on P2P (Peer-to-peer) -arkkitehtuuri.

3 KOKEEN TOTEUTUS

Työssä tutkittiin omalla työasemalla virtuaaliympäristössä pfSense-palomuuria, joka perustuu avoimeen lähdekoodiin. Lisäksi etsittiin tietoturva-aukkoja oman asiakasohjelmiston sekä Nessus Vulnerability Assessment-ohjelmiston avulla. Asiakasohjelmisto etsii avoimia portteja kotiverkosta.

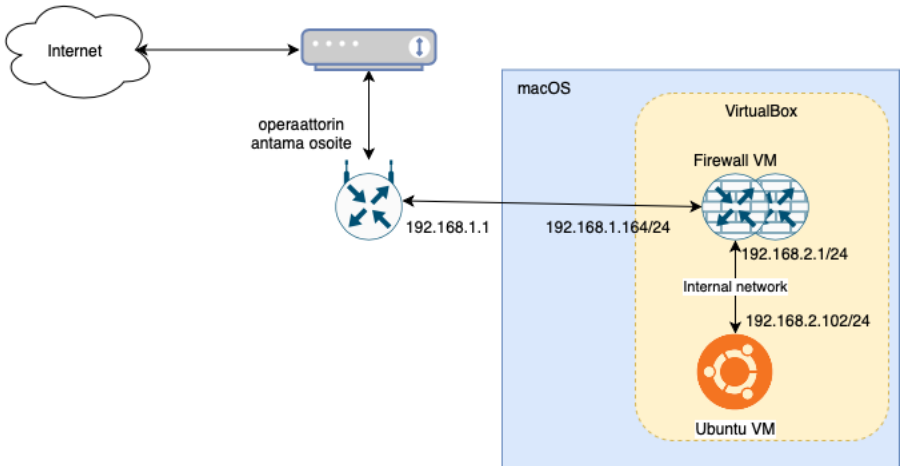
3.1 Virtuaalinen testiympäristö

Työssä luotiin omalle työasemalle (Macbook Pro /macOS Big Sur) virtualisoitu ympäristö, jossa voitiin kokeilla palomuurikäyttöön soveltuvia avoimen lähdekoodin verkkopalomuureja ilman, että hankittiin erillistä laitetta niitä varten. Virtualisointiin käytettiin Oraclen tarjoamaa ilmaista VirtualBox-ohjelmaa, joka on saatavissa Windows-, Linux- ja macOS- käyttöjärjestelmille.

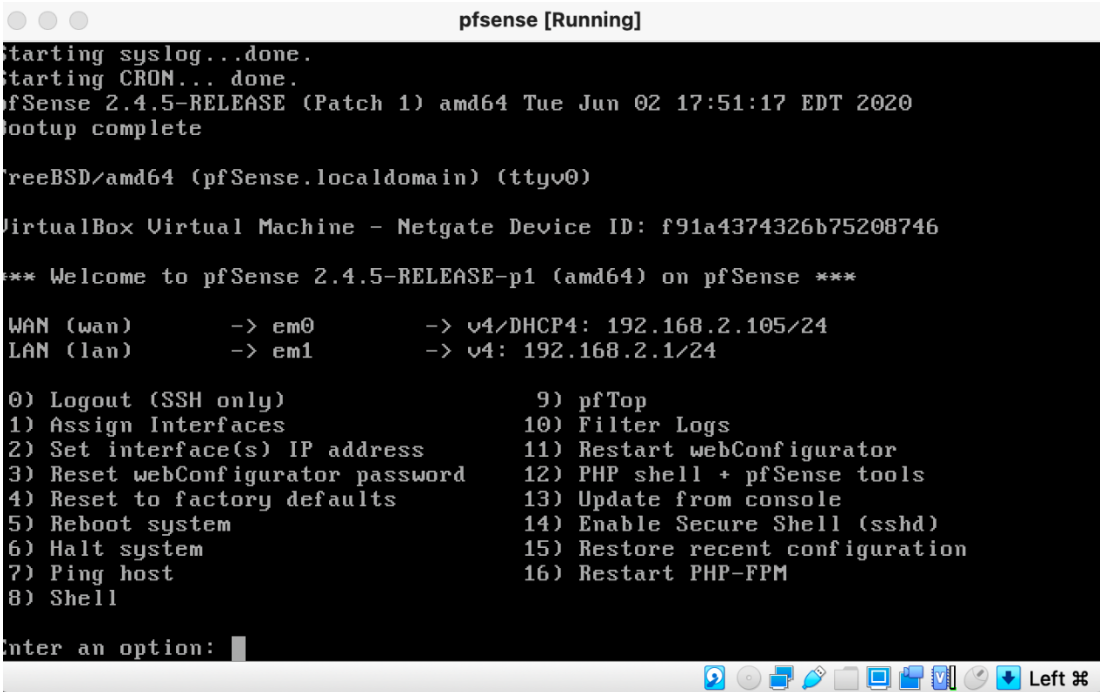
3.2 Testiympäristön asennus

pfSenseä kokeiltiin VirtualBox-ympäristössä. pfSense asennettiin verkkosivuilta, jossa on upotettu ohjevideo asentamiseen. Ohjelmasta valittiin eurooppalainen toisinto ja CD-asentaja (ISO). [37]

pfSense-virtuaalikone konfiguroitiin niin, että sen WAN-rajapinnaksi asetettiin kotiverkko ja LAN-rajapinnaksi asetettiin virtuaalikoneen sisäinen verkkorajapinta. Testiä varten asennettiin lisäksi Ubuntu-virtuaalikone, jonka verkkoyhteytenä on virtuaalikoneen sisäinen verkkorajapinta. Verkko-osoitteet allokoitiin sekä kotiverkossa että pfSensen alla olevassa sisäisessä verkossa DHCP:llä. Ubuntu-koneella ei ollut omaa kotiverkossa näkyvää IP-osoitetta vaan sen liikenne kulki NAT:in läpi. pfSense käytti sillattua adapteria WAN-yhteydelle (l. yhteys kotiverkon reitittimeen, alla kuvassa 192.168.1.1) ja LAN-yhteydelle oli siinä sisäinen verkko. Kuvissa 8 ja 9 ovat verkkopalomuurin testausympäristö sekä pfSensen päävalikko. Kuvissa 10–12 on kuvakaappauksista erilaisista pfSensen asetuksista.



Kuva 8. Verkkopalomuurin testaus. Reitittimestä kulkee yhteys MacOS:iin, jossa on virtuaalinen Ubuntu-ympäristö ja pfSenseVM.



Kuva 9. pfSensen päävalikko ja WAN/LAN-asetukset

3.3 pfSensen sääntöjen testaus

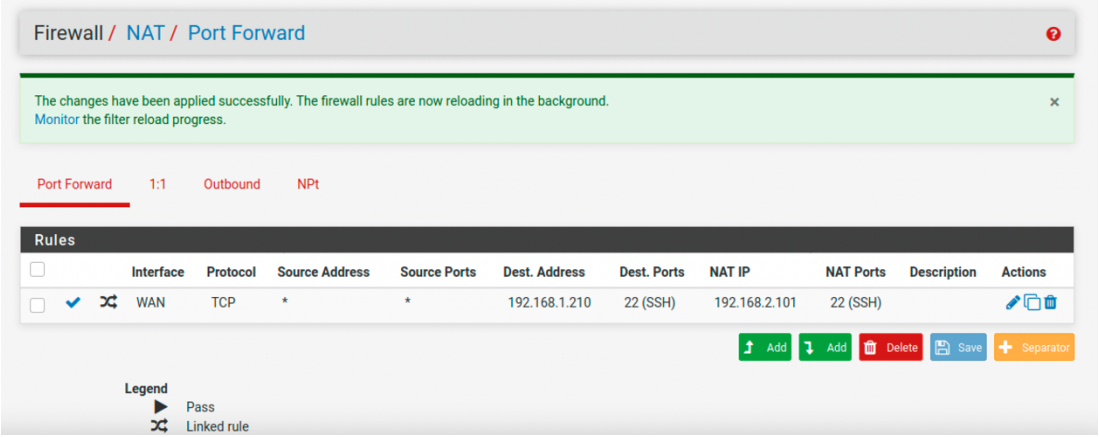
PfSensessä on 64-bittinen BSD (Berkeley Software Distribution) -käyttöjärjestelmä ja sitä hallitaan web-käyttöliittymän avulla. Käyttäjä voi määritellä omat palomuurisäännöt pfSenseen.

Kuvissa 10, 11 ja 12 on esimerkkejä verkkopalomuurin säännöistä.
pfSenseä testattiin erilaisilla asetuksilla tulevalle liikenteelle:

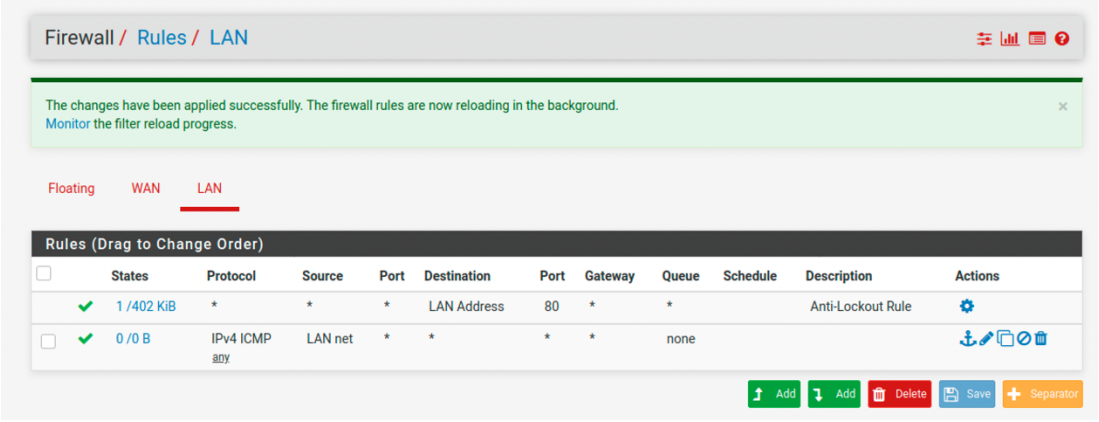
- kaikki tuleva liikenne estetty,
- vain ICMP (ping) sallittu ja
- portinsiirto Ubuntu-koneella olevalle palvelulle (ssh))

Vastaavasti lähtevälle liikenteelle tehtiin seuraavat säännöt:

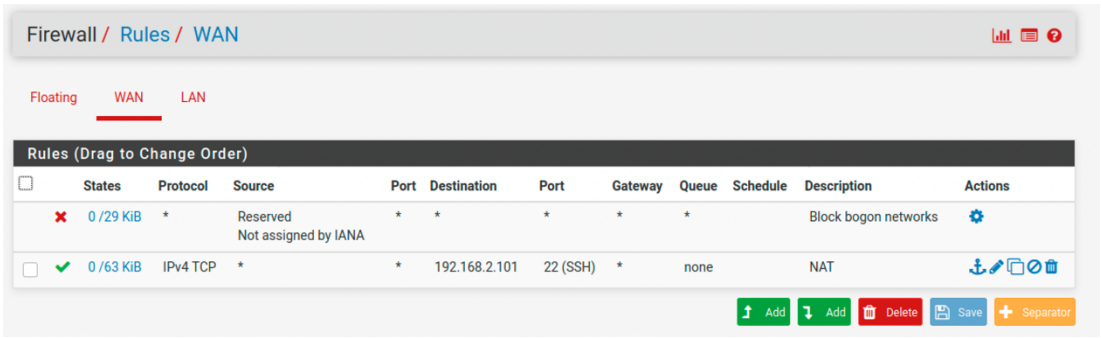
- kaikki estetty,
- kaikki sallittu ja
- vain ssh, https, DNS ja ICMP sallittu



Kuva 10. Esimerkki palomuurisäännöstä pfSensessä. Portinsiirtoasetuksella sallittu SSH testiympäristön Ubuntu-palvelimelle.



Kuva 11. LAN:in säännöissä on määrätty, että lähtevä ICMP on sallittu.



Kuva 12. Palomuuri sallii SSH:hon lähtevää liikennettä.

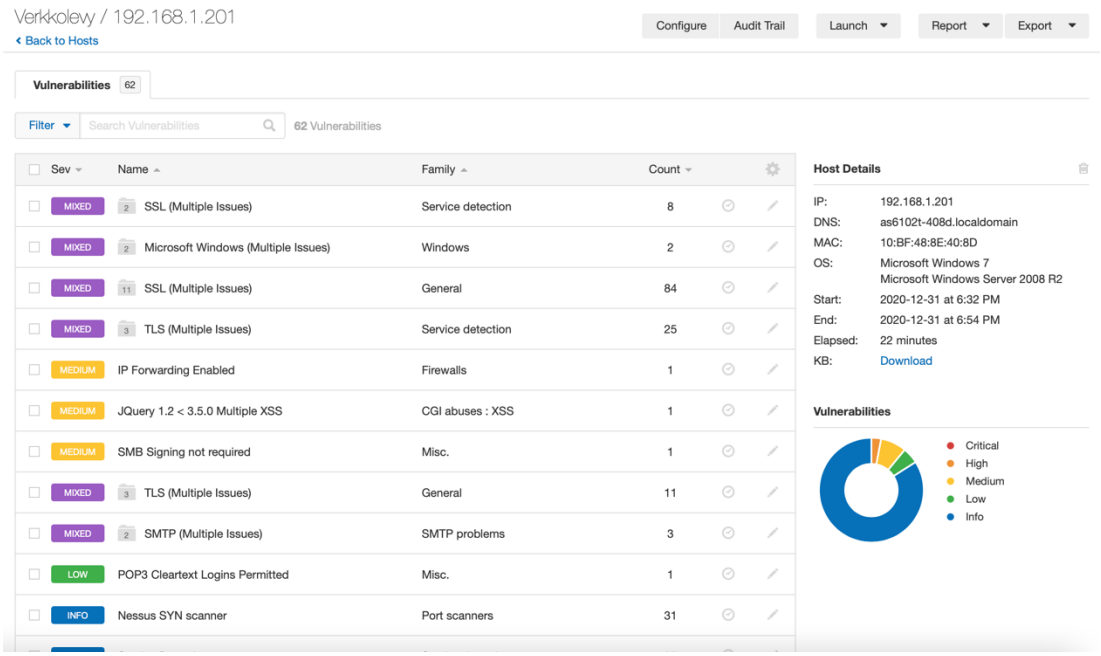
3.4 Kotiverkon ja palomuurien testaus

Palomuurien suojausta testattiin pfSensestä ja yleisesti kotiverkosta.

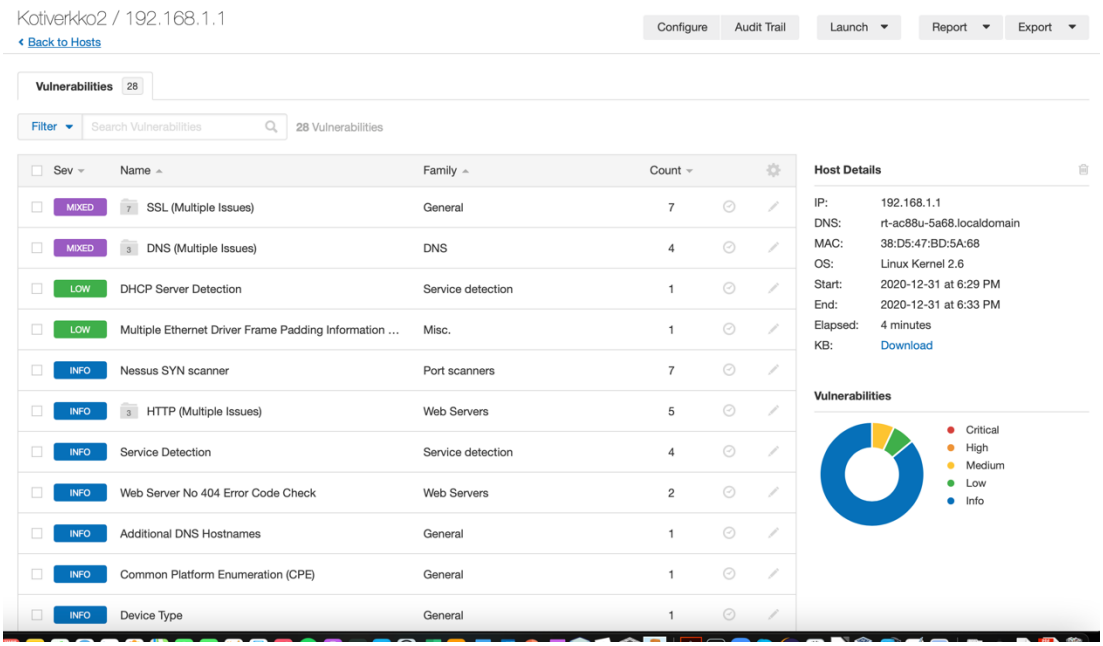
Työssä toteutettiin lisäksi Python 3:lla pieni asiakasohjelmisto, jolla voi tarkistaa halutusta IP-osoitteesta tai -aliverkosta auki olevat TCP-portit ja varmistaa palomuuriasetusten toiminnan. Ohjelma käyttää socket- ja datetime-kirjastoja. Lisäksi ohjelma käyttää IPNetwork-kirjastoa. Ohjelma ajetaan komennolla ./main.py.

Ohjelma ajaa ping-komennon kaikille kotiverkon palvelimille, jos ei ole yksittäistä palvelinta valittuna. Jos yksittäinen palvelin valitaan, ping-komentoa ei suoriteta. Ohjelma käy palvelimet läpi minimiportista maksimiporttiin ja etsii niiden IP-osoitteet ja ne, jotka vastaavat, näyttävät avoimet TCP-portit ja joita ei ole suojattu palomuurilla.

Lisäksi palomuuria testattiin Nessus Vulnerability Assessment -ohjelmiston avulla. Nessus Vulnerability Assessmentissa on web-käyttöliittymä ja se paljastaa haavoittuvuuksia valitusta palvelimesta [24]. Siinä on luokittelu haavoittuvuuksille vakavuuden mukaan. Haavoittuvuuksia tarkistettiin kotiverkon reitittimeltä ja verkkolevyltä. Niistä ei löytynyt kriittisiä haavoittuvuuksia. Kotiverkossa ei ole julkiseen internetiin auki olevia portteja, mikä kävi ilmi ajamalla testejä kotireitittimeltä löytyvään julkisen verkon osoitteeseen. Kuvissa 13–14 näkyy Nessus-ohjelman löytämiä uhkia.



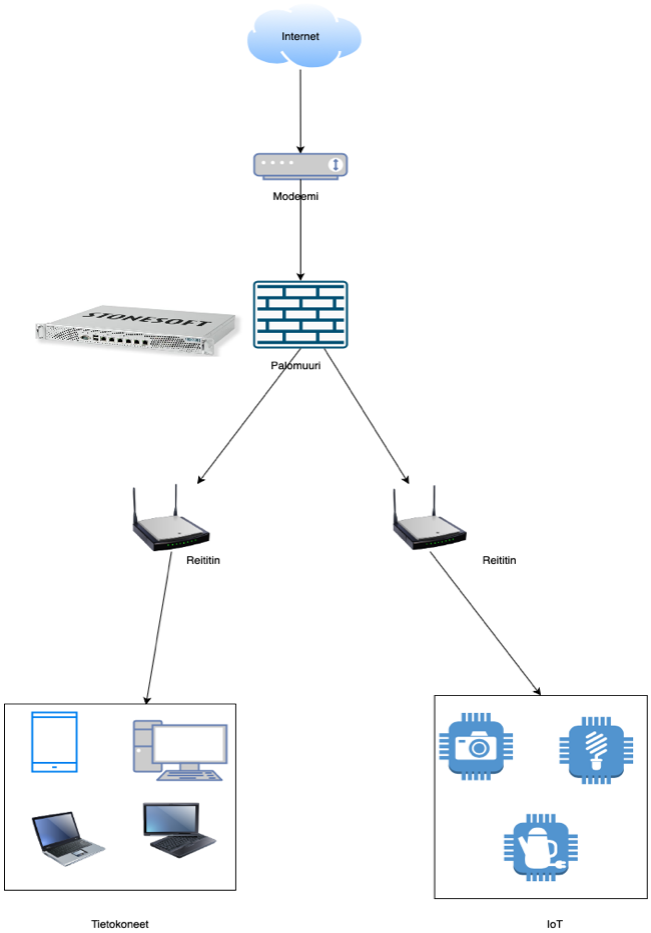
Kuva 13. Verkkolevyn uhkia



Kuva 14. Kotiverkon uhkia

4 POHDINTAA

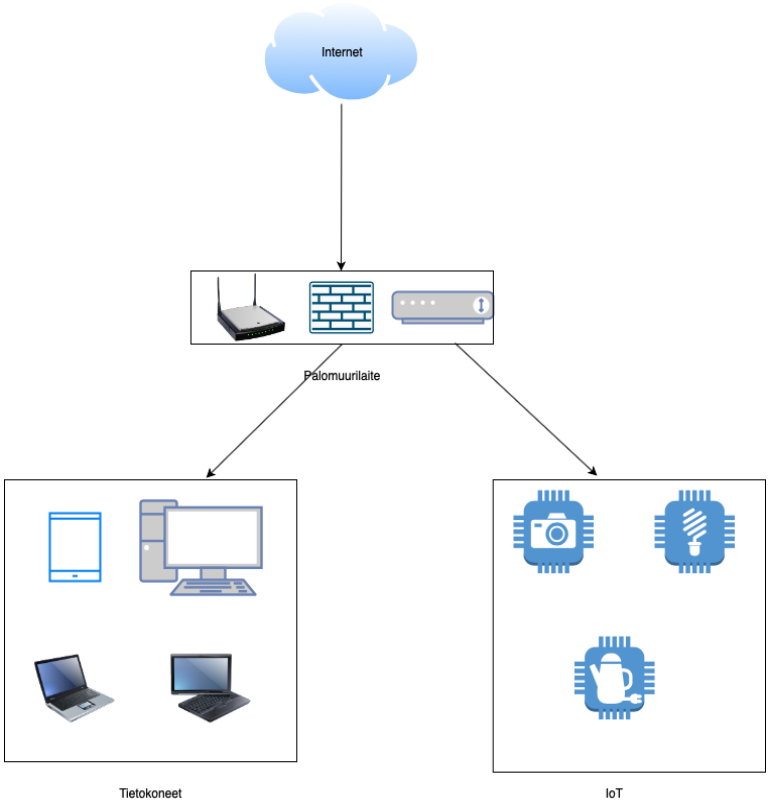
Kuvan 15 verkossa on erillinen palomuuri, joka voidaan toteuttaa mini-PC:llä ja avoimen lähdekoodin palomuurilla. Kotiverkon laitteet on mahdollista jakaa erillisiin aliverkoihin. Esimerkiksi internetistä käytettävät laitteet kuten NAS (Network-attached storage) -levyt ja IOT-laitteet sijoitetaan toiseen aliverkkoon ja loput laitteet toiseen, turvalliseen aliverkkoon.



Kuva 15. Kotiverkon rakenne: Internetistä tulee liikennettä kotiverkkoon. Modeemi on ennen erillistä palomuurilaitetta ja reitittimiä.

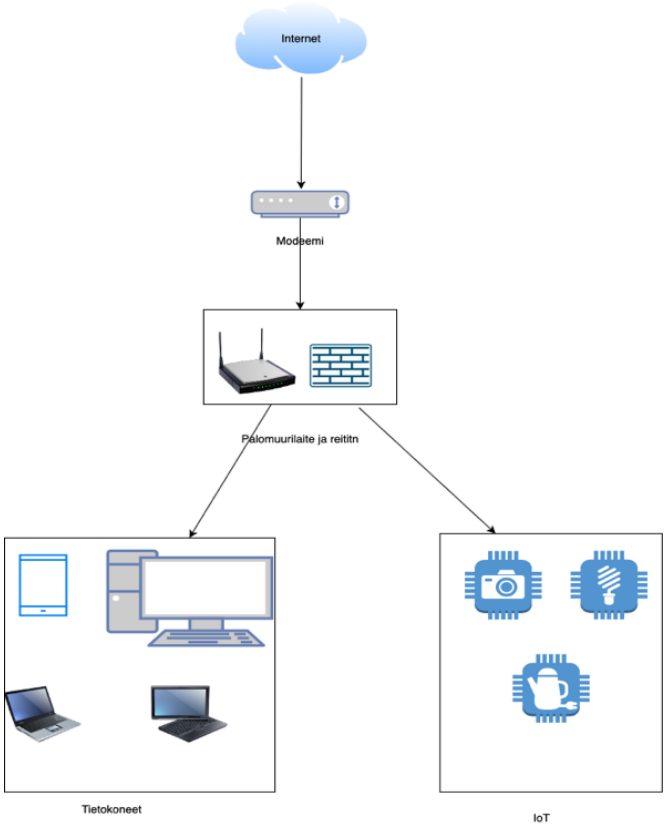
Erillisen verkkopalomuurin hankkiminen voisi olla hyödyllistä siinä tilanteessa, ettei verkkolaitteissa ole ennestään kunnollista palomuuria. Kuitenkin esimerkiksi pfSensen käyttö vaatii komentojen ja eri palomuurisääntöjen konfiguroinnin opettelemista. Tavalliselle kotikäyttäjälle tämä voi olla hankalaa.

Palomuuri, reititin ja modeemi voivat olla kuvan 16 mukaisesti yhdessä monitoimilaitteessa. Esimerkiksi operaattorin toimittamassa kaapelimodeemissa voi olla modeemiominaisuuden lisäksi langaton reititin ja palomuuri. Tällöin erillisen reitittimen tai palomuurin hankintaa ja hallintaa ei tarvita. Palomuuri- ja reititinominaisuudet kuitenkin ovat rajoitetumpia kuin erillislaitteilla. Monitoimilaitteessa palomuuri ei yleensä sisällä mitään IDS/IPS-ominaisuuksia. [38, 39]



Kuva 16. Kotiverkon rakenne, jossa yhdessä monitoimilaitteessa on modeemin lisäksi reititin ja palomuuri.

Kotiverkko on mahdollista toteuttaa kuvan 17 mukaisesti myös niin, että hankkii modeemin lisäksi erillisen reitittimen, jossa on monitoimilaitetta monipuolisemmat reititin- ja palomuuriominaisuudet. Operaattorin toimittama monitoimilaite on mahdollista konfiguroida pelkäksi modeemiksi asettamalla se siltaavaan toimintamoodiin ja kytkemällä langattoman reitittimen pois käytöstä. Joissakin kotiverkkoon soveltuvissa reitittimissä voi olla IDS/IPS-ominaisuuksia, joilla tietoturvaa saa parannettua. [22]



Kuva 17. Kotiverkon rakenne, jossa reitittimessä on palomuuriomaisuudet. Modeemi on erillisenä laitteena.

Jerusalemin yliopiston ja Frauenhof-instituutin tutkimuksien [31, 32] mukaan esimerkkejä reitittimien ongelmista ovat päivittämättömyys, puuttuvat pääsytiedot ja oletuspääsytiedot. Erillinen, avoimella lähdekoodilla toimiva verkkopalomuuri on erittäin todennäköisesti päivitettävissä pitempään kuin kotiverkkoon hankittu reititin. Esimerkiksi pfSense on ollut käytössä vuodesta 2004 saakka ja siihen on tullut koko ajan päivityksiä.

pfSensen ominaisuudet toimivat hyvin eri käyttötarkoituksissa. Palomuuri-ominaisuudet ovat selvästi laajemmat ja täydellisemmin hallittavissa kuin tavanomaisessa kotiverkon reitittimessä. Erillisellä palomuurilla on mahdollista jakaa kotiverkko aliverkkoihin ja hallita palomuurisäännöillä näiden välistä liikennettä. IDS/IPS-ominaisuudetkin olisi tällaiseen palomuuriin mahdollista toteuttaa esimerkiksi Snort- tai Suricata-moduulilla. Erillinen laite kuitenkin aiheuttaa ylimääräisiä kustannuksia ja vaatii hallintaa.

Mikäli kotiverkon verkkopalomuurin haluaisi toteuttaa avoimen lähdekoodin ohjelmistolla, pitäisi sitä varten hankkia joko laite, jossa kyseinen ohjelmisto on valmiiksi asennettuna (esim. NetGate) tai sitten yleiskäyttöinen mini-PC, johon ohjelmiston voisi itse asentaa. Mini-PC:n tulisi täyttää ohjelmiston vaatimukset:

- Riittävän tehokas suoritin, jossa prosessorin käskykannassa tuki salaukselle (Advanced Encryption Standard New Instructions, AES-NI),
- Muistia esimerkiksi 2GB, jos haluaa asentaa IDS/IPS:n ja riittävästi kiintolevyä.
- Vähintään kaksi 1 Gbps porttia – toinen ”ulkoverkon” WAN-liitännälle ja toinen kotiverkon LAN-liitännälle. Portteja tarvitsee enemmän, jos koti-verkkoa haluaa jakaa osiin.

5 YHTEENVETO

Supon vuonna 2021 julkaisemasta kybervakoilutiedotteesta selviää, että kotiverkko on erityisen herkkä rikollisuuden ja vakoilun kohde. Supo ei turhaan varoita suomalaisia. Erityisesti koronapandemian aikana kybervakoilu on lisääntynyt.

Työn tavoite oli tutkia kotipalomuurien tietoturvaa ja sen parantamista, jotta tällaisia uhkia voitaisiin ehkäistä. Kokeellisessa osassa testattiin pfSenseä virtuaalisessa Ubuntu-ympäristössä ja etsittiin tietoturva-aukkoja kotiverkosta oman asiakasohjelmiston ja Nessus Essentials Vulnerability Scanner -ohjelmiston avulla. Huomattiin, että pfSensen sääntöjen konfigurointi voi aluksi olla hankalaa kotikäyttäjälle ja vaatii perehtymistä. Oman asiakasohjelmiston avulla voi löytää avoimia portteja kotiverkosta, mutta Nessus Essentials Vulnerability Scannerilla näkee yksityiskohtaisemmin, mitä uhkia kotiverkossa on. Oma asiakasohjelmisto tehtiin Python 3:lla.

Tietoturvan kehittämiseksi reitittimien ja muiden verkkoon liitettyjen laitteiden asetuksia tulee tarkkailla ja päivittää säännöllisesti. Myös Nessus Essentials Vulnerability Scannerilla tai muilla ohjelmistoilla on hyvä selvittää kotiverkon uhkia. Erillinen palomuurilaite kannattaa hankkia, jos verkkolaitteissa itsessään ei ole kunnollista palomuuria. Palomuuri ei yksin riitä suojaamaan tietyiltä uhilta, kuten bottiverkoilta tai tietokoneviruksilta. Sen takia bottiverkkoihin liittyvissä tutkimuksissa yritetäänkin löytää uusia tekniikoita tällaisten uhkien torjumiseen.

6 LÄHTEET

1 McGill, Tanya & Thompson, Nik (2017) Old risks, new challenges: exploring differences in security between home computer and mobile device use. In: Taylor and Francis Group.

2 CISA: Security Tip (ST15-002) URL: https://us-cert.cisa.gov/ncas/tips/ST15-002 Viitattu 25.3.2021

3 Supo: Ulkomaiset tiedustelupalvelut käyttävät yritysten ja yksityishenkilöiden verkkoreitittimiä kybervakoiluun URL: https://supo.fi/-/ulkomaiset-tiedustelupalvelut-kayttavat-yritysten-ja-yksityishenkiloiden-verkkoreitittimia-kybervakoiluun Viitattu 25.3.2021

4 Ingham, Kenneth & Forrest, Stephanie (2002) A History and Survey of Firewalls

5 Johdatus tietoliikenteeseen Osa 2 URL: https://johdatus-tietoliikenteeseen-19.mooc.fi/osa-2 Viitattu 25.3.2021

6 Michael Mullins: Exploring the anatomy of a Data Packet (2001) URL: https://www.techrepublic.com/article/exploring-the-anatomy-of-a-data-packet/ Viitattu 25.3.2021

7 The User Datagram Protocol (UDP) URL: https://erg.abdn.ac.uk/users/gorry/course/inet-pages/udp.html Viitattu 25.3.2021

8 What is NAT URL: https://support.huawei.com/enterprise/en/doc/EDOC1100086645 Viitattu 25.3.2021

9 ASUS FAQ URL: https://www.asus.com/fi/support/FAQ/1037906 Viitattu 25.3.2021

10 Talal et al. (2019) A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home. In: IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.9, September 2019 pp.138-146

11 Eastom Chuck (2018) Network Defence and Countermeasures, Third Edition. Pearson Edition, Inc.

12 Data Encapsulation and the TCP/IP Protocol Stack URL: https://docs.oracle.com/cd/E19683-01/806-4075/ipov-32/index.html Viitattu 25.3.2021

13 TKK: Henkilökohtaiset palomuurit URL: https://www.netlab.tkk.fi/opetus/s38118/s00/tyot/44/palomuurit.shtml Viitattu 25.3.2021

14 IDS vs IPS: What is the Diffence URL: https://www.varonis.com/blog/ids-vs-ips/ Viitattu 25.3.2021

15 Antoon W. Rufi A (2006) Chapter 1: Vulnerabilities, Threats and Attacks. Network Security 1 & 2 Company Guide pp.1-47

16 Dandamundi, Sahithi S & Eltaeib, Tarik (2015) Firewalls Implementation in Computer Networks and their role in Network Security.

17 Webopedia: Windows Firewall URL: https://www.webopedia.com/definitions/windows-firewall/ Viitattu 25.3.2021

18 Tietoja ohjelmapalomuurista URL: https://support.apple.com/fi-fi/HT201642 Viitattu 25.3.2021

19 LinuxWiki: Palomuuri: URL: https://www.linux.fi/wiki/Palomuuri Viitattu 25.3.2021

20 Linux firewalls: What you need to know about iptables and firewalld URL: https://opensource.com/article/18/9/linux-iptables-firewalld Viitattu 25.3.2021

21 Mohammad Forhad Iftekher: Iptables vs Firewalld URL: https://www.unixmen.com/iptables-vs-firewalld/ Viitattu 25.3.2021

22 Asus FAQ: How does AiProtection protect my network URL: https://www.asus.com/support/FAQ/1012070/

23 8 Best Open Source Firewall to Protect Your Network URL: https://geekflare.com/best-open-source-firewall/

24 Metasploit URL: https://www.metasploit.com Viitattu 25.3.2021

25 Moore, Micahel D. (2017) Penetration Testing and Metasploit

26 Nessus URL: https://www.tenable.com/products/nessus Viitattu 25.3.2021

27 Discovery scan URL: https://docs.rapid7.com/metasploit/discovery-scan/ Viitattu 25.3.2021

28 Matt Danda (2017) Hacking a Home Network

29 Yaqoob et al. (2017) Penetration Testing and Vulnerability Assessment. In: Journal of Network Communications and Emerging Technologies (JNCET) Volume 7, Issue 8, August (2017)

30 Voronkov et al. (2017) Usability of Firewall Configuration. In: ACM Computing Surveys, Vol. 50, No. 6, Article 87. Publication date: December 2017.

31 Weidenbach Peter & Vom Dorp, Johannes (2020) Home Router Security Report 2020

32 Rotenberg et al. (2017) Authentication-Bypass Vulnerabilities in SOHO Routers In: SIGCOMM Posters and Demos '17, August 22–24, 2017, Los Angeles, CA, USA pp.66-68

33 Hafeez et al. (2015) Securebox: Toward Safer and Smarter IoT Networks

34 Hafeez et al. (2017) Securing Edge Networks with Securebox

35 Mailewa et al. (2019) SECURITY THREATS/ATTACKS VIA BOTNETS AND BOTNET DETECTION & PREVENTION TECHNIQUES IN COMPUTER NETWORKS: A REVIEW

36 Ullah et al. (2013) Survey on botnet: Its architecture, detection, prevention and mitigation

37 Pfsense download URL: https://www.pfsense.org/download/ Viitattu 25.3.2021

38 DNA: Kaapelilaajakaistan asennus ja käyttö URL: https://www.dna.fi/documents/753910/853489/20171204_DNA_Kaapelilaajakaista_Asennus-ja-kaytto_Opas_A4_low.pdf/b6d42cf5-6843-4b67-9d68-9542d8e5d3c2 Viitattu 25.3.2021

39 Telia: Technicolor CGA-kaapelimodeemin käyttöohje https://www.telia.fi/asiakastuki/laitteet/technicolor-cga2121 Viitattu 25.3.2021